## Claims

Having thus described the invention, what is claimed is:

1. A computerized method having a process flow operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and executing at least one of the activities in the process flow, the method comprising the steps of:

assembling an electronic authorization of a transaction;

extracting verifiable role certificates from said electronic authorization; and

verifying whether role certificates, associated with the authorization, are themselves authentic.

2. The method of claim 1 wherein roles associated with the role certificates are hashed and compared with hashed roles in a database of hashed roles.

3. The method of claim 1 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

4. The method of claim 3 wherein the authorization structure is an authorization tree.

5. The method of claim 3 wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and

hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

6. A distributed workflow management system, the management system operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and executing at least one of the activities in a process flow, the system comprising:

code for assembling an electronic authorization of a transaction;

code for extracting verifiable role certificates from said electronic authorization; and

code for verifying whether role certificates, associated with the authorization, are themselves authentic

7. The system of claim 6 wherein roles associated with the role certificates are hashed and compared with hashed roles in a database of hashed roles.

8. The system of claim 6 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

9. The system of claim 8 wherein the authorization structure is an authorization tree.

10. The system of claim 8 wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be

compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

11. A computerized method having a process flow operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and executing at least one of the activities in the process flow, the method comprising the steps of:

assembling an electronic authorization of a transaction;

extracting verifiable role certificates from said electronic authorization; and

verifying whether role certificates, associated with the authorization, are themselves authentic.

12. The method of claim 11 wherein roles associated with the role certificates are hashed and compared with hashed roles on a database of hashed roles.

13. The method of claim 11 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

14. The method of claim 13 wherein the authorization structure is an authorization tree.

15. The method of claim 13 wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

16. A distributed workflow management system, the management system operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and executing at least one of the activities in a process flow, the system comprising:

code for assembling an electronic authorization of a transaction;

code for extracting verifiable role certificates from said electronic authorization; and

code for verifying whether role certificates, associated with the authorization, are themselves authentic.

17. The system of claim 16 wherein roles associated with the role certificates are hashed and compared with hashed roles in a database of hashed roles.

18. The system of claim 16 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

19. The system of claim 18 wherein the authorization structure is an authorization tree.

20. The system of claim 18, wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

21. A Transaction Authorization Method encoded on a computer readable medium, the method having the following steps:

(a) receiving a request for a transaction;

(b) obtaining an electronic representation of a document having details of the transaction from a Digital Document Database;

(c) obtaining the role certificate signed with a signature by a Transaction Administrator from a Role Certificate Database and verifying the signature;

(d) returning the transaction details to the requester;

(e) awaiting and receiving from the requester the completed representation, signed by the requester;

(f) requesting the Authorization Structure for the transaction from the Authorization Structure Database, the Authorization Structure being pre-signed with a signature by the Transaction Administrator and verifying the signature, and choosing a permission set of role names and user members of the permission set to contact to sign in these role names;

(g) forwarding details of the transaction request with the signature of the requester to others having roles corresponding to the chosen permission set and collecting signatures of each role indicated in the permission set;

(h) requesting role certificates from the Role Certificate Database and signatures for each member of the permission set and encoding the same on the document; and

(i) forwarding the completed electronic document including the signatures and role certificates to the requester, the document including authorization details required in order to confirm the validity of the transaction.

22. The method of claim 21 wherein the role certificates and the Authorization Structure consist of hashed information about permission sets and roles, such hashed information substituting for the unhashed role certificates and permission sets.

23. A Transaction Verification Method encoded on a computer readable medium, the method having the following steps:

(a) receiving an electronic document representing a transaction, associated transaction details being signed by a Transaction Authority, a collection of role certificates certifying named roles signed by a Role Authority, the transaction details signed by each of the signing keys corresponding to the verification keys in the role certificates, and the Authorization Structure;

(b) using a verification key of the Role Authority to check each certificate on the document;

(c) in the following manner, checking the signatures on the transaction details using the verification keys in the supplied role certificates:

i. extracting the named roles from the role certificates;

ii. hashing the roles using a hash-of-hashes process ;

iii. checking the computed hash value of the transaction against that was originally signed by the Transaction Authority to ensure that it is equal to the value for the transaction received in the Authorization Structure;

iv. using the output of the hash-of-hashes process as input to check the signature on the hash-of-hashes process; if the produced hash-of-hashes string matches the hashed string signed by the Transaction Authority, then assuming that the request is authorized; and

(d) reporting the result.

24. A distributed workflow management system encoded with a Transaction Authorization Method, the method having the following steps:

(a) receiving means for receiving a request for a transaction;

(b) retrieving means for obtaining an electronic representation of a document having details of the transaction from a Digital Document Database;

(c) retrieving means for obtaining the role certificate signed with a signature by a Transaction Administrator from a Role Certificate Database and verifying the signature;

(d) transmission means for returning the transaction details to the requester;

(e) receiving means for receiving from the requester the completed representation, signed by the requester;

(f) querying means for requesting the Authorization Structure for the transaction from the Authorization Structure Database, the Authorization Structure being pre-signed with a signature by the Transaction Administrator;

(g) verifying means for verifying the signature;

(h) selection means for choosing a permission set of role names and user members of the permission set to contact to sign in these role names;

(i) transmission means for forwarding details of the transaction request with the signature of the requester to others having roles corresponding to the chosen permission set and collecting signatures of each role indicated in the permission set;

(j) retrieving means for requesting role certificates from the Role Certificate Database and signatures for each member of the permission set;

(k) encoding means for encoding the signatures gathered in step (j) on the document; and

(l) transmission means for forwarding the completed electronic document including the signatures and role certificates to the requester, the document including authorization details required in order to confirm the validity of the transaction.

25. The system of claim 24 wherein the role certificates and the Authorization Structure consist of hashed information about permission sets and roles, such hashed information substituting for the unhashed role certificates and permission sets.

26. A distributed workflow management system encoded with a Transaction Verification Method, the method having the following steps:

(a) receiving an electronic document representing a transaction, associated transaction details being signed by a Transaction Authority, a collection of role certificates certifying named roles signed by a Role Authority, the transaction details signed by each of the signing keys corresponding to the verification keys in the role certificates, and the Authorization Structure;

(b) using a verification key of the Role Authority to check each certificate on the document;

(c) in the following manner, checking the signatures on the transaction details using the verification keys in the supplied role certificates:

i. extracting the named roles from the role certificates;

ii. hashing the roles using a hash-of-hashes process ;

iii. checking the computed hash value of the transaction against that was originally signed by the Transaction Authority to ensure that it is equal to the value for the transaction received in the Authorization Structure;

iv. using the output of the hash-of-hashes process as input to check the signature on the hash-of-hashes process; if the produced hash-of-hashes string matches the hashed string signed by the Transaction Authority, then assuming that the request is authorized; and

(d) reporting the result.

27. A message exchange mechanism operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and being able to read and write messages to be sent to another resource over the computer network, the mechanism performing the steps of:

assembling an electronic authorization of a transaction;

extracting verifiable role certificates from said electronic authorization; and

verifying whether role certificates, associated with the authorization, are themselves authentic.

28. The mechanism of claim 27 wherein roles associated with the role certificates are hashed and compared with hashed roles in a database of hashed roles.

29. The mechanism of claim 27 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

30. The mechanism of claim 29 wherein the authorization structure is an authorization tree.

31. The mechanism of claim 29 wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

32. A message exchange mechanism operating over a computer network comprising a plurality of interconnected computers and a plurality of resources, each computer including a processor, memory and input/output devices, each resource operatively coupled to at least one of the computers and executing at least one of the activities in a process flow, the system comprising:

code for extracting role certificates of at least one type from a message; and

code for verifying if said role certificates, associated with the authorization, are themselves authentic.

33. The mechanism of claim 32 wherein roles associated with the role certificates are hashed and compared with hashed roles in a database of hashed roles.

34. The mechanism of claim 32 wherein the authorization is further insured by verifying that role certificates associated with the authorization correspond with roles in a permission set of roles of an authorization structure, the role certificates of which being required to authorize the transaction.

35. The mechanism of claim 34 wherein the authorization structure is an authorization tree.

36. The mechanism of claim 34, wherein the roles are extracted from the role certificates associated with the transaction, each extracted role being hashed and these hashed roles being concatenated and hashed again, and then concatenated with hashes of other permission sets, if any, according to the authorization structure and hashed once again, resulting in a computed hash value which may be compared to that which was signed by the Transaction Administrator, a match indicating that the transaction is authorized.

Page 36 of 96